Development and Piloting of a Software Tool to Facilitate Proactive Hazard and Risk Analysis of Health IT

Ibrahim Habli (University of York)
Yan Jia (University of York)
Sean White (NHS Digital)
George Gabriel (University of York)
Tom Lawton (Bradford Royal Infirmary and Bradford Institute for Health Research)
Mark Sujan (University of Warwick)
Clive Tomsett (Cerner Corporation)

Abstract

Health Information Technology (HIT) is now widely promoted as a means for improving patient safety. The technology could also, under certain conditions, pose hazards to patient safety. However, current definitions of hazards are generic and hard to interpret, particularly for large HIT in complex socio-technical settings, i.e. involving interacting clinical, organisational and technological factors. In this paper, we develop a new conceptualisation for the notion of hazards and implement this conceptualisation in a tool-supported methodology called the Safety Modelling, Assurance and Reporting Toolset (SMART). SMART aims to support clinicians and engineers in performing hazard identification and risk analysis and producing a safety case for HIT. Through a pilot study, we used and examined SMART for developing a safety case for electronic prescribing in three acute hospitals. Our results demonstrate the ability of SMART to ensure that the safety evidence is generated based on explicit traceability between the clinical models and HIT functionality. They also highlight challenges concerning identifying hazards in a consistent way, with clear impact on patient safety in order to facilitate clinically-meaningful risk analysis.

Keywords: Health IT, Patient Safety, Hazards, Risks, Electronic Prescribing

Acknowledgements

This work was supported, in part, through a grant by the UK Royal Academy of Engineering (ISS1516\8\8) and a PhD Fellowship by the Yorkshire and Humber Patient Safety Translational Research Centre. We are grateful to colleagues who supported SMART and this study: Alistair Morris, Kay Pagan, Paul Southern, Beve Smith, Jackie Murphy, Hannah Mccann, Wale Lawal, Chris McLernon and Damon Horn.

1 Introduction

The introduction of Health Information Technology (HIT) can have positive and negative impact on patient safety [1, 2, 3]. In this paper, we focus on the potential hazards and associated risks rather than on the expected benefits. In this regard, different international and national standards and initiatives have emphasised the importance of adopting safety risk management principles for the design and deployment of HIT [4, 5, 6]. These typically are centred on an explicit description of the technology and its context, the identification of the hazards and the assessment and management of the risks associated with these hazards during the design, use and maintenance of the technology [7, 8].

The systematic and proactive implementation of these principles is well understood and established in traditional engineering domains such as aviation and nuclear power [9]. In such domains, the technology, procedures and organisations are well defined and controlled, as are the system boundaries and interfaces. This enables focused hazard identification and risk analysis [10].

However, the above cannot be assumed in healthcare [11]. This is mainly due to the inherent complexity, flexibility and scale of healthcare services, some of which are irreducible, e.g. varying the care in order to suit patients with different clinical conditions, together with individual and social needs and constraints [12]. This, in turn, complicates the safety analysis processes for HIT. Such processes require a clear and structured description of the clinical environment within which the technology is deployed [13]. These safety processes focus on two notions: hazards and risks.

A hazard is defined as "*a potential source of harm to a patient*" [14] while a risk is the "*combination of the severity of harm to a patient and the likelihood of occurrence of that harm*" [14]. In an environment in which harm and risk are predominantly caused by the clinical conditions and the complexity of clinical practice, identifying technology-related hazards and associated risks is easier described than realised. That is, especially in critical care and cases involving chronic diseases or comorbodities, the risk to patients due to clinical complications and complex clinical decisions, e.g. whether to operate or not, often outweighs the risk caused by technology-related errors, e.g. late retrieval of electronic records. In such a high-risk environment, there is a significant challenge in identifying, justifying and agreeing on a set of potential sources of harm posed by HIT [15]. In other words, there are many different ways in which HIT could fail to meet its intended purpose (e.g. due to usability, hardware, software and network errors). The challenge lies in identifying and prioritising a subset of these failure modes that could lead to a clinical hazard and compromise patient safety.

Despite its central role in safety processes, the concept of hazard is loosely defined in the safety literature. The above definition by NHS Digital in England is consistent with the definition offered by the International Organization for Standardization (ISO) of a hazard as a "*potential source of harm*" [16]. This is also the same as the definition provided by the International Electrotechnical Commission (IEC) in the generic functional safety standard IEC 61508 [17]. Beyond healthcare, in aviation, the US Federal Aviation Administration (FAA) defines a hazard as a "*condition that could foreseeably cause or contribute to an aircraft accident*" [18]. In defence, the UK Ministry of Defence defines a hazard as a "*physical situation or state of a system, often following from some initiating event, that may lead to an accident*" [19]. In the academic literature, Leveson refines existing definitions by emphasising the role of the environment. She defines a hazard as a "*system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss)*" [20]. Although all of the aforementioned definitions agree on hazards as sources, states, conditions or situations that can lead to harm, they do not provide criteria that can help reduce the generic scope of the term, and hence to identify hazards in practice.

Our recent review of HIT safety practices in England [56] supports this view, highlighting that the "*identified HIT hazards, and their associated risks and controls, are rarely specific to the system and the clinical environment, or justified in sufficient detail, to enable the stakeholders to evaluate and, where necessary, challenge the safety beliefs about the system*" [56]. It is important to note that, like hazards, there is much debate about risk and the way in which it has been approached from different perspectives [21, 22].

In this paper, we present a tool-supported methodology for supporting proactive and systematic hazard identification and risk analysis for HIT. In particular, our paper considers three questions:

Q1. What is a consistent and clear conceptualisation of hazards for HIT?
Q2. How can this conceptualisation be implemented?
Q3. To what extent is treating hazard as a central concept useful for HIT safety analysis?

In order to answer Q1, we developed a new conceptualisation for hazards for HIT building on our review of hazard identification practices and existing definitions of hazards in safety standards and the literature. For Q2, we implemented this conceptualisation in a tool-supported methodology called the Safety Modelling, Assurance and Reporting Toolset (SMART)[1]. SMART aims to support clinicians and engineers in modelling the clinical, organisational and technological aspects, in an integrated manner, and performing hazard identification and risk analysis for HIT. For Q3, through a pilot study, we used and examined SMART, and its underpinning hazard conceptualisation, for developing a safety case for electronic prescribing in three acute hospitals and discussed and reflected on the lessons learnt from different technical and clinical perspectives.

The rest of paper is organised as follows. In Section 2, we present our conceptualisation of hazards for HIT. In Section 3, we introduce SMART as a tool-supported methodology for implementing this conceptualisation. In Section 4, we present a pilot study on the use of SMART for analysing the safety of electronic prescribing in three acute hospitals. In Section 5, we discuss our results and explore the strengths and weaknesses of our approach. Finally, in Section 6, we present our conclusions.

2 Conceptualising Hazards for HIT

The list of hazard definitions discussed in Section 1 shows a lack of clarity, focus and consistency in how the fundamental concept of hazard is described. Building on the results and recommendations in the recent review of HIT safety practices by Habli et al [56], we define the following criteria for the concept of hazards as a basis for improving hazard identification practices for HIT:

(1) The impact of a hazard on patient care is clear: A hazard should be primarily clinically oriented and not technologically oriented in order to show the relevance of the hazard to patient harm. This is fundamental, particularly for determining severity during risk analysis [14, 16]. For example, the loss of power sources for a HIT system is a significant failure and a potential source of many hazards. However, it is not a hazard because the link to patient harm is neither clear nor necessarily direct. However, a late diagnosis or a wrong prescription are hazards because the potential clinical impact is relatively easy to determine (e.g. disease progression or unintended drug interactions). That is, diagnosis and prescribing hazards are conditions of the diagnosis and prescribing processes, and not the technological processes (although the technology is potentially a major contributory factor). As such, these hazards exist in clinical practices prior to the deployment of the digital solution and should equally apply to paper-

[1] The toolset is available to download at https://www.cs.york.ac.uk/safedh/SMART.html

based solutions. With the introduction of a HIT system, some of the existing clinical hazards will start to emerge through, and on the interface of, the HIT functionality, e.g. electronically issuing a wrong prescription.

(2) Hazards occur on the boundaries of the clinical systems: hazards are system-level conditions. As such, a clear and consistent definition and characteristics of the different clinical systems and their contextual settings is fundamental, including how and the extent to which the HIT functionality supports these systems at the boundary level (Figure 1). For example, the setting being analysed might comprise one national system, e.g. electronic referrals, or a set of independent yet interrelated medication management systems, e.g. electronic prescribing, preparation, administration, monitoring and reconciliation systems. The responsibility of each of these clinical systems, and the associated system hazards, primarily lies with the relevant and accountable clinical authority, e.g. physicians, pharmacists or nurses. Currently, hazards are defined either at a too low level to reflect potential harm to patients or very genericly to enable a clear and meaningful link to the clinical environment [56].

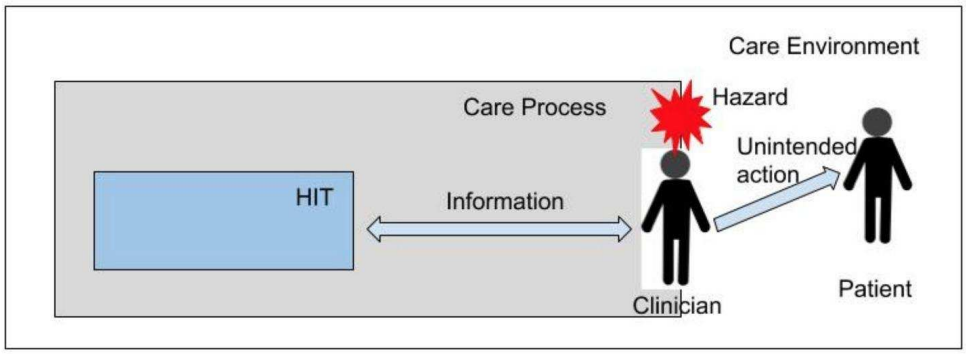


Figure 1: System Boundary

(3) The position of a hazard should allow sufficient space for detection and mitigation: hazards are useful concepts in that if they are controlled, the risk of different types of harm is reduced. The positioning of the hazards should ensure that neither the hazard nor its potential harm are inevitable. That is, controls can be put in place to detect and mitigate failures and faults that can lead to the hazard. Equally, controls can be deployed to detect and mitigate the transition from the hazard to potential patient harm. This is often represented in the form of a bowtie diagram [23] (Figure 2). In this regard, safety standards for HIT, e.g. those provided by the NHS, emphasise the need to distinguish between existing and additional controls for detecting and mitigating the causes and effects of the hazards [14].

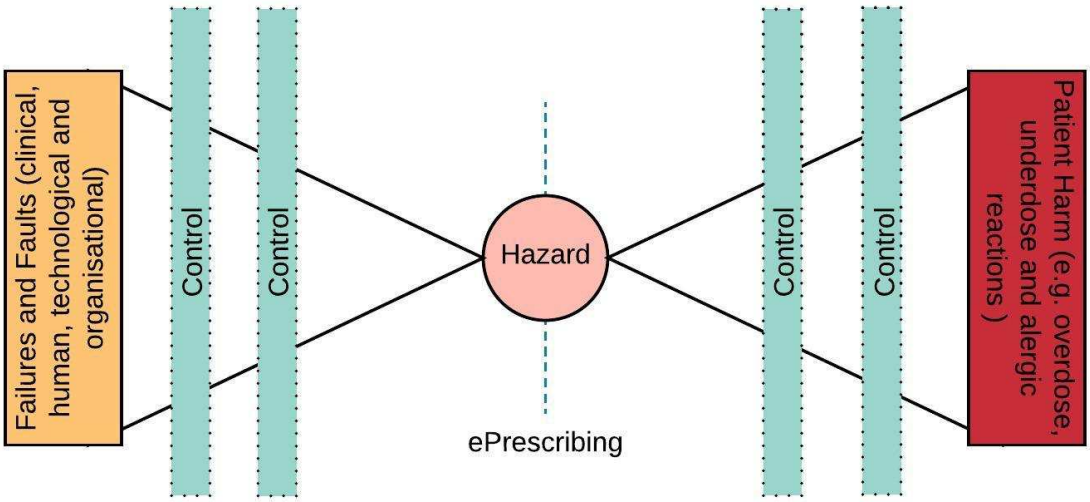


Figure 2: Bowtie Diagram

(4) Hazards are major failure conditions but not all major failure conditions are hazards: consider a significant event such as the complete loss of IT or shortage of clinical staff. These do not necessarily constitute a hazard. Rather, these are common causes for many hazards and can often even be more dangerous than a single clinical hazard. These common causes should be identified and managed through different techniques and processes (e.g. using Fault Trees [24]). Labeling every single major condition as a hazard could result in an excessively large Hazard Log, and dilute the effort available for managing genuine hazards. It could also lead to information overload and inconsistent hazard definitions (i.e. hazards at different levels of granularity).

3 SMART: Tool-Supported Methodology for Hazard Identification and Risk Analysis

A fundamental aspect of the above conceptualisation is the linkage between the clinical processes and settings on the one hand and the HIT functionality on the other hand. A hazard associated with the technology cannot be identified, and its risk analysed, in isolation from the healthcare setting.

To support the above and to operationalise the hazard conceptualisation in Section 2, we developed the Safety Modelling, Assurance and Reporting Toolset (SMART). SMART provides a self-contained platform for developing explicit clinical safety cases for HIT [5]. A safety case documents an argument, based on the evidence i.e. mainly based on hazard identification and risk analysis, for why the system is considered to be safe for a given application in a given environment [14]. In SMART, the safety analysis is clinically driven through a structured model of the clinical processes and an explicit description of the care settings.

The development of SMART has been model driven, based on the Eclipse Modelling Framework (EMF) [28], which provided the basic structure of the Java code. The core aspects of the data model are described in Section 3.2. The development of the toolset has been agile and iterative, allowing continuous feedback from the clinical users, representing NHS Digital and different healthcare providers and technology firms. The primary users of the tool are the Clinical Safety Officers (CSOs) [14] who, in their capacity as experienced clinicians, are expected to lead the HIT risk management activities. CSOs are typically supported by a team of clinicians, engineers and analysts.

From a methodological perspective, SMART implements the hazard conceptualisation by supporting three central HIT risk management activities [14]:

- Modelling the clinical context and the HIT system, ensuring that (1) the clinical setting, including the decision making process and the flow of clinical activities, (2) the HIT functions and (3) the mapping between the clinical setting and HIT functions are explicitly defined;
- Identifying hazards in the modeled clinical setting, ensuring that the hazards associated with the HIT functions are explicitly traced to the contextual factors;
- Analysing the risks associated with the identified hazards, showing how these risks, and their control measures, could vary across different clinical settings and HIT functions.

These activities are described in the next 3 sections, with emphasis on the explicit interlinks between the clinical and technological factors, including the underlying SMART data model and the key user-interface aspects of the tool design.

3.1 Clinical Context and HIT Modelling

Central to the design of SMART is a graphical flow-charting interface through which a clinical process of activities and decisions can be modelled. This is in essence similar to process mapping with which clinicians are already familiar. The diagrams produced using the toolset represent the sequence of steps that a patient may encounter as they progress through the care system (Figure 3). We refer to these diagrams as "Care Processes", and it is through them that the core information for Hazard Identification and Risk Analysis is collected (i.e. safety in the clinical context). This simple representation provides an expressive means for describing pathways of care while being simple and intuitive enough to use with little training. Within a care process, an activity represents some action carried out in a health or social care setting. In order to ensure specificity in the identification of HIT-related hazards, the care process editor in SMART allows activities and decisions to be associated with particular HIT functions. The HIT systems and their associated functions are defined by the user in a separate section of SMART – the 'System Editor'. SMART also allows the user to define "Care Settings", which describe and correspond to services and locations, e.g. Maternity Unit or Pharmacy, that a patient may visit or use during the process of receiving care. A setting may be associated with an activity/decision in the Care Process, thus providing additional context for the activity/decision, e.g. the level of staffing or noise in the defined setting.

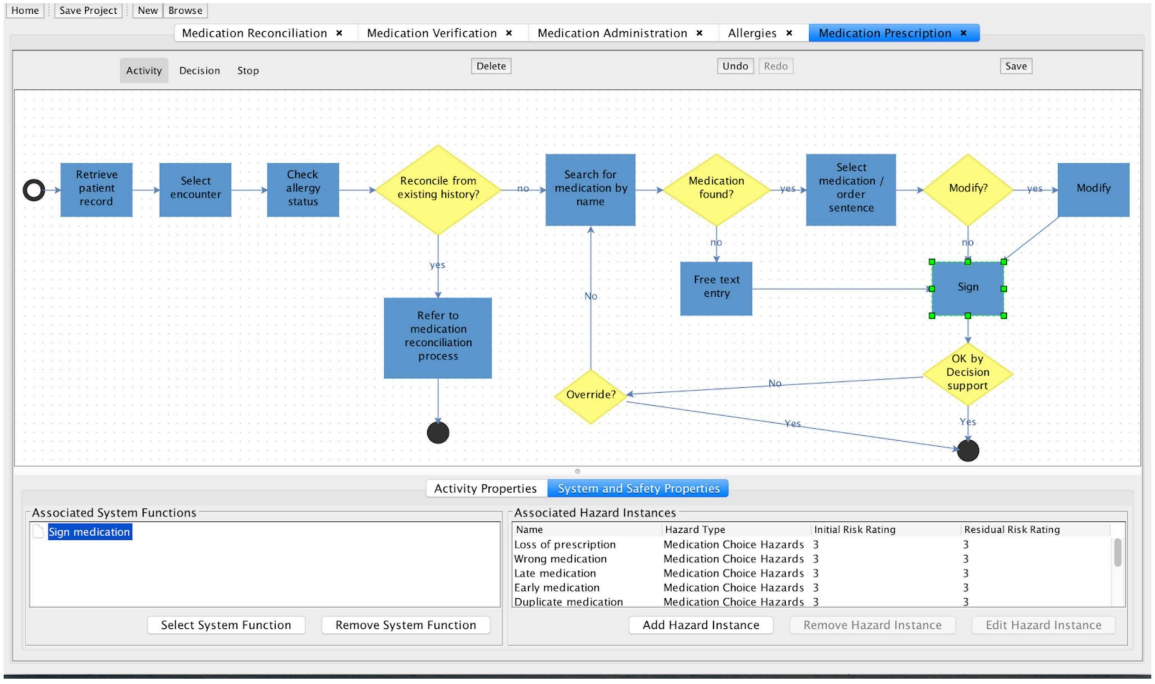


Figure 3: SMART Care Process Model

3.2 Hazard Identification

Within SMART, the concept of a hazard is decomposed into two related aspects. Firstly, the user may create "Hazard Types" with no reference to the context within which they may occur (e.g. late prescription or wrong dose). Secondly, the user can associate a "Hazard Instance" to any Hazard Type. Instances are specific occurrences of the hazard defined by the associated Hazard Type. To enforce contextualisation of Hazard Instances, they must be associated with both an Activity or Decision in a Care Process and a System Function. In effect, this ensures that Hazard Instances are only discussed in a specific context (e.g. 'wrong dose prescribed by an Obstetrician in a Maternity ward'), thereby helping to provide a shared contextual understanding about the relative risk of a hazard. The degree of specificity in describing the relevant contextual factors will inevitably depend on the clinical setting and the stage at which the analysis is performed (i.e. during design or deployment). For instance, a high-level description of a hazard as 'wrong dose prescribed in secondary care' might be sufficient for a technology firm to allow the engineers to design holistic controls such as automated rules for dose range checking. However, once a HIT system is selected for deployment in a specific clinical setting, the clinicians and engineer will have to be more detailed in the description of the contextual factors, e.g. 'wrong dose of *insulin* prescribed for a *pregnant diabetic* women by an Obstetrician in a Maternity ward'. This might allow the health organisation to deploy additional controls that suit the specific clinical context, e.g. varying the degree of dose cross-checking depending on medication or the experience of the prescriber.

In essence, in SMART, a Hazard Instance is a product of four components:

Hazard Instance = Hazard Type x Clinical Setting x Clinical Step x System function.

The above is shown in the SMART data model extract in Figure 4, and illustrated in grey. The model, defined in the Unified Modelling Language (UML) [25], specifies the relationships between the primary concepts in SMART. A Hazard Instance has mandatory links with a Hazard Type and a Clinical Step (which in turn has to be associated with a Clinical Setting). A Hazard Instance has a link with a System Function, which can be optional in order to allow the identification of non-HIT related Hazard Instances. It is important to note that SMART, in this respect, aims to ensure

that the necessarily types of links are established. However, it is neither possible nor desirable for the tool to dictate the content of the hazard description, especially as the analyses and the safety case are expected to evolve in an incremental manner as a collaboration between the engineers and clinicians.

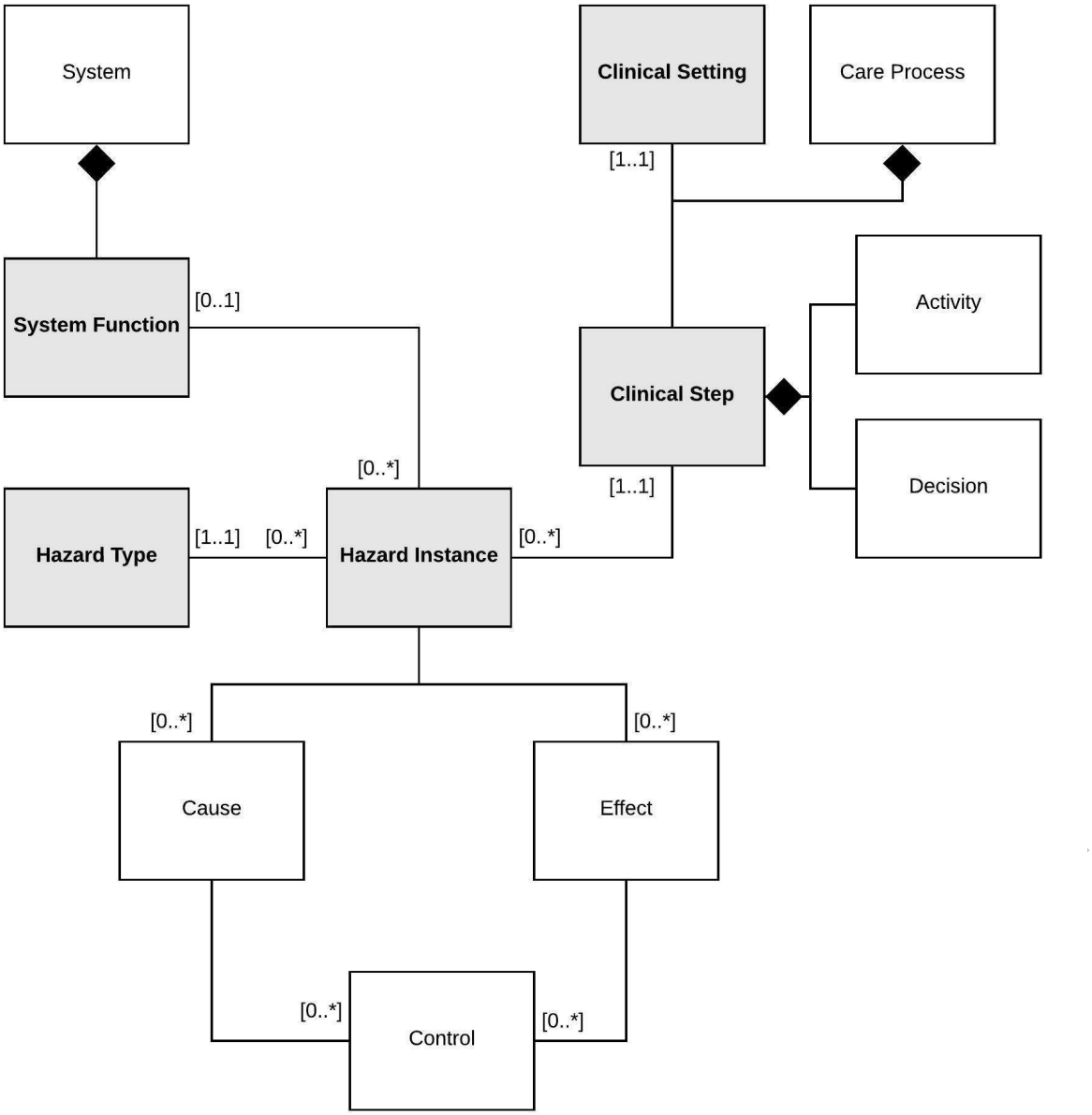


Figure 4: Data Model Extract

3.3 Risk Analysis

Hazard Instances are associated with several other pieces of information. Severity and likelihood ratings must be specified for all Hazard Instances, hence determining the level of risk, typically based on a Risk Matrix, i.e. determining the level of risk based on the likelihood of the harm against the potential severity of the harm. It is important to identify the difference between initial and residual risk ratings. Initial risk ratings are those which describe the hazard instance before the implementation of controls. Residual risk ratings define the same three elements (severity, likelihood and risk) after the implementation of controls. Much of this data corresponds to the entries in the "Hazard Log" section of the clinical safety case report template developed by NHS Digital [14]. Thus, with the addition of some extra information provided in

another integrated editor, SMART automatically generates and exports conformant reports using the data from modelling and analysis in the tool.

3.4 Traceability

The traditional approach of presenting HIT safety evidence as written clinical safety case reports or spreadsheets makes it difficult to understand the connections between various components of the analysis. SMART's data model was structured to ensure that the logical relationships between the model components as depicted in Figure 4 are automatically established and managed. All of the data is user defined as they require expertise and judgement of both clinical and engineering staff. However, by enforcing these relationships, the inherent structure of dependencies between the constituent parts of the hazard and risk analysis is clarified.

Although SMART insists on specifying, as a minimum, a care setting, a care process, a HIT function and a hazard type as a prerequisite for declaring a hazard instance (i.e. in order to ensure that the hazard instances are clinically meaningful and traceable), the approach is flexible in the level of detail that a user enters in describing care settings and processes, leaving it to the user to select an appropriate sociotechnical model [26, 27] and the granularity of the clinical activities and decisions, considering the complexity and criticality of the HIT deployment.

4 Pilot Study

As we are interested in the impact on practice, a pilot study, through an actual in-depth experience, is best suited for exposing the strengths and weaknesses of the hazard conceptualisation and its implementation in SMART. Essentially, we are interested in identifying and examining insights from the use of SMART, i.e. hurdles, mitigations and workarounds, as well as sharing the outcomes of the tool, i.e. list of hazards and associated risks.

4.1 Study Overview

The initial evaluation of SMART included the use of the approach to develop safety cases for two HIT systems in four large acute hospitals, one national clinical service, one app and one telehealth platform. In this paper, we describe a HIT deployment in acute care, covering three hospitals, in which SMART was used in the Hazard Identification and Risk Analysis for an electronic Prescribing and Allergies Management (ePAM) system.

Medication management was selected as it is one of the most safety-critical processes in healthcare [29]. Increasingly, the process is supported by HIT, covering the different phases, mainly prescribing, preparation and verification, administration and monitoring, including supporting activities for reconciliation and allergies management. Both the potential safety benefits and risks associated with HIT for medication management are highlighted in the literature [30, 31]. Here, we limit the scope to analysing and managing the safety risks of ePAM. More specifically, we examine how proactive and systematic Hazard Identification and Risk Analysis, supported by SMART, can generate the evidence in order to support an explicit safety case for a complex socio-technical ePAM. The system is selected not on its own unique merits but because it represents a typical use of HIT, supplied by an external technology firm, in order to support prescribing and allergies management as part of a wider HIT deployment, e.g. including electronic health records.

Eight multidisciplinary workshops were organised, including a meeting dedicated for planning. The purpose of these workshops was to identify the hazards and analyse the risks associated with the deployment of ePAM. SMART was used as the primary approach for driving the analysis and recording the outcomes, i.e. producing a Hazard Log for ePAM. The

multidisciplinary team included 3 clinical consultants, 2 nurses, 2 pharmacists, 2 safety engineers, 2 researchers and 2 systems engineers (representing the HIT supplier). All the clinicians have clinical lead roles in the overall HIT deployment project. The workshops were used to satisfy three fundamental requirements of the safety standard SCCI 0160, which is mandated by NHS England: (1) defining the scope of the system, including the clinical settings, (2) identifying hazards to patients and (3) estimating and evaluating risks before and after the deployment of risk control measures. The analysis is based on a critical reflection about our experiences with the use of SMART for proactive HIT hazard identification and risk analysis. Critical reflection is a frequently used technique to learn from experience and to improve practice [32, 33].

4.2 Using SMART for the Safety Analysis of ePAM

The results are grouped based on the application of SMART to define the clinical scope and system (Section 4.1.1) and perform hazard identification (Section 4.1.2) and risk analysis (4.1.3).

4.2.1 Scope Definition

The scope of the analysis is Electronic Prescribing, including allergies management, in its clinical context. As such, the first challenge was to describe the relationship between prescribing, as a clinical activity, and Electronic Prescribing, as a digital information system. This was seen as essential in order to highlight that hazards caused by clinical factors were outside the scope of the analysis, e.g. hazards due to an incorrect clinical decision. That is, Electronic Prescribing is one of many interrelated human, social and technological systems that are used to support prescribing. Figure 5 shows the main modules covered by medication management, including prescribing and allergies management. These modules define the clinical scope within which the HIT functionality is used.

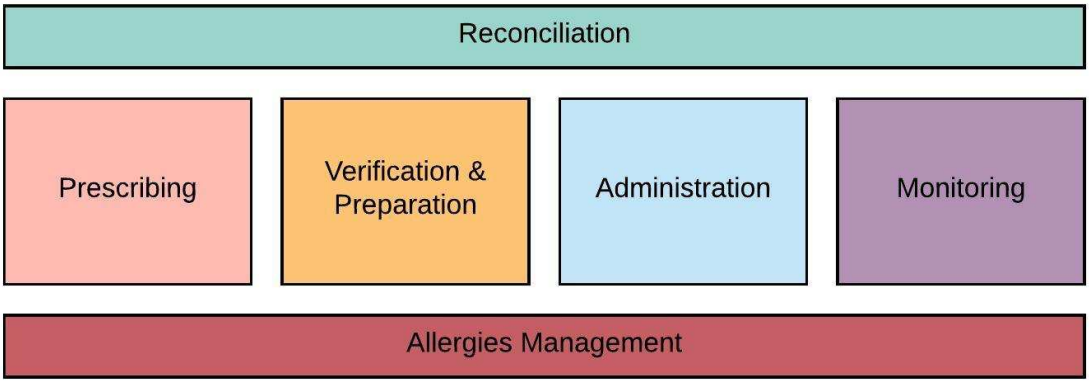
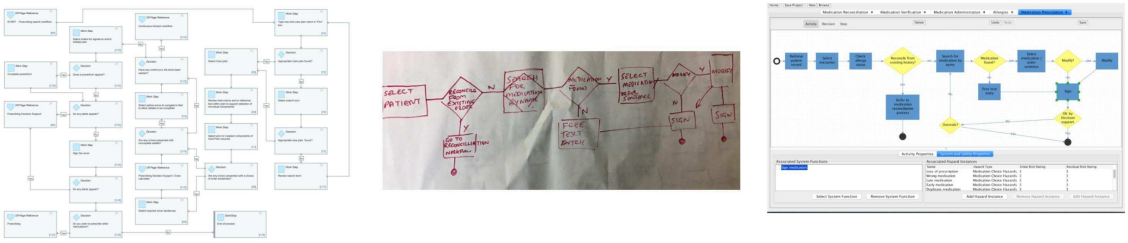


Figure 5: Medication Management Overview

Prior to this study, models of the clinical processes existed, created through an exercise of mapping clinical practices and HIT functionality. However, for the purpose of Hazard Identification, this was seen as too detailed and IT-centric, e.g. 'click to approve' or 'right click for more options'. Further, many of these process models were generated based on predefined templates provided by the supplier. As a result, in order to improve the validity of the processes and emphasise the clinical focus of the Hazard Identification, the multidisciplinary team re-created the clinical process models to describe the flow of activities and decisions as perceived and performed by the users, i.e. healthcare staff. Figure 6 shows the transition from (A) a detailed IT-centric process model to (B) a refined model created manually by the clinical team and (C) a further refinement of the model by the multidisciplinary team in SMART that formed the basis for the Hazard Identification.



(A) Initial Process Model (B) Refined Process Model by Clinical Team (C) Final Model used for Hazard Identification

Figure 6: Refinement of Care Process Models

Concerning the care settings in which ePAM is used, the following were specified: (1) Inpatient, (2) Outpatient, (3) Pharmacy and (4) Community. Each of the process steps in the care models had to be associated with a specific care setting. Finally, 18 different HIT functions were specified for ePAM. Importantly, these functions were specified from the user perspective (i.e. making it clear how they serve a clinical purpose). A subset of these functions is listed in Table 1.

HIT Function Name	**Description**
Document Medication	Record in the patient's health record the medication that has been prescribed
Continue Medication	Record in the patient's health record that a decision has been made to continue with the medication that has been prescribed
Discontinue Medication	Record in the patient's health record that a decision has been made to discontinue the medication that has been prescribed
Modify Medication	Modify an existing medication
Add Allergy	Add a new medicine allergy to patient's health record
Modify Allergy	Modify an existing medicine allergy in the patient's health record
Record 'Unable to Obtain Allergies'	Record in the patient's health record that patient's allergies have not been obtained in support of the prescribing activity
Sign	Sign prescription, taking responsibility for the appropriateness of the prescribed medication and completeness of the prescription

Table 1: HIT Prescribing Functions

At the end of this phase, each HIT function was explicitly traced to specific clinical activities and decisions and the settings within which it is used. This provided a basis for identifying the main *touch points* between the technology and its specific clinical context.

4.2.2 Hazard Identification

The starting point for Hazard Identification was to agree on an overall hazard classification that is clinically meaningful. We classified the hazards associated with prescribing through ePAM into 5 types :

1. Medication *Choice* Hazards
2. Medication *Dose* Hazards
3. Medication *Route* Hazards
4. Medication *Time* Hazards

5. Patient *Identification* Hazards.

These types are based on the five rights in medication safety [34]. Allergies management is a critical issue in the medication process. A hazard such as 'prescribing a medication to which a patient is allergic' can have severe consequences [35]. The team had two options, either to consider this hazard under the 'Medication Choice Hazards', i.e. wrong medication, or create a new type, i.e. 'Allergies Hazards'. The team adopted the latter option in order to highlight the significance of this type of hazard, which is consistent with hospital policy, and the National Institute for Health and Care Excellence (NICE) and Medicines and Healthcare products Regulatory Agency (MHRA) guidance concerning allergies [36, 37].

Next, each type was refined further based on the failure classes defined in the Software Hazard Analysis and Resolution in Design (SHARD) method [38, 44], which is a variant of the process industries' Hazard and Operability Study (HAZOP) technique [39]. These failure classes are: *Omission*, *Commission*, *Early*, *Late* and *Incorrect*. That is, these failure classes, when applied to a Hazard Type, refined the hazard conditions into specific Hazard Instances. For example, Table 2 shows the Hazard Instances associated with the Medication Choice Hazards type.

Type: Medication Choice Hazards	
Failure Classes	**Hazard Instances**
Omission	Medication not prescribed when intended.
Commission	Medication prescribed when not intended.
Early	N/A - Early signing activity addressed within Commission
Late	N/A - Late signing activity addressed within Omission
Incorrect	Wrong medication prescribed Duplicate medication prescribed Adverse interaction

Table 2: Medication Choice Hazards, Failure Classes and Instances

In order to declare a Hazard Instance for ePAM, the context had to be clearly defined in terms of the clinical settings and steps. This was performed based on the clinical processes described in the Scope Definition section. For example, in the prescribing process model (Figure 3), a number of Hazard Instances were declared against the activity of digitally signing a prescription. This clinical activity results in issuing an electronic prescription. An electronically signed prescription is on the boundary between multiple systems and authorities, i.e. typically prescribing by doctors, verification by pharmacists, and preparation by nurses.

The Hazard Identification of ePAM is consistent with both the medication error classification based on the medication process (prescribing, transcribing, dispensing, administering and monitoring) [42] and that based on the type and modality, which are often referred to as "five rights" [43]. In this particular case, type and modality helped provide a detailed characterisation of the hazard, e.g. adverse interaction. The classification based on the medication process helped describe the context of the hazard, e.g. *clinician prescribed* a medication that has adverse interaction with an existing medication. This is important as it enables the safety analysts to deploy risk controls which are relevant to the specific phase in which the hazard might occur [45, 46], e.g. prescribing risk controls as opposed to administration risk controls.

4.2.3 Risk Analysis

At this stage, the causes and effects of the Hazard Instances were identified, considering human, organisational and technological factors, but excluding clinical factors. Importantly, using SMART, this analysis was performed given the specific clinical context associated with the Hazard Instance, i.e. the already defined activity/decision in a specific care process within a specific care setting and using a specific HIT function. This helped ensure that the causes and effects were relevant to the Hazard Instance. This also helped ensure that the risk estimation and evaluation, including any necessary controls, were performed given the relevant contextual factors.

The risk of each Hazard Instance was then estimated, based on the *the severity of harm and the likelihood of occurrence of that harm* , e.g. the likelihood that the patient suffers a permanent life-changing incapacity as the result of the medication overdose. Deciding on the likelihood and severity parameters was a challenging task [40, 41]. For example, for the Hazard Instance 'prescribing a medication to which the patient is allergic ', it is likely that there will be relatively little harm (e.g. no reaction, or a mild rash etc), but there is a very low (but non-zero) likelihood of a severe harm (e.g. death). The current likelihood and severity parameters makes it difficult to reconcile the fact that a Hazard Instance could result in death, but is more likely to result in minor/no harm. Essentially we found ourselves wanting to subdivide these categories.

Each risk was then evaluated against predefined acceptability criteria, e.g. as defined in the risk matrix provided by NHS Digital. Next, options were identified and analysed for controlling the risks that were deemed unacceptable, e.g. through training and supervision. Figure 7 shows an example Hazard Instance Form in SMART, covering Causes, Effects and Controls and including traceability to the Hazard Type, HIT Function and Care Process Step.

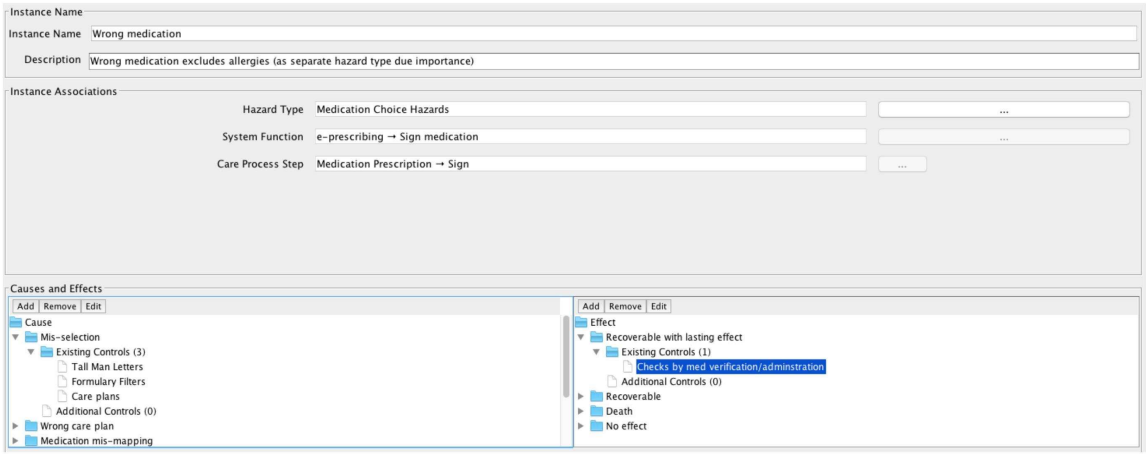


Figure 7: SMART Risk Analysis

5 Discussion

In this research, we provided four criteria for refining the notion of hazards, combined with SMART as a modelling methodology and toolset. The four criteria helped ensure that the hazards identified are clinically meaningful, particularly in how they relate to patient care and clinical practice. SMART builds on these principles by creating a platform that brings together clinical and technology models as a prerequisite and a structured basis for Hazard Identification and Risk Analysis. In this Section, we discuss the main findings of the pilot and the overall strengths and weaknesses of SMART.

5.1 Analysis of ePAM using SMART

We report on the key findings of the ePAM Hazard Identification and Risk Analysis that we performed using SMART. The findings are described against the four criteria for hazard conceptualisation that are discussed in Section 2.

Clarity of the Impact on Patient Care

Deciding on how and when the technology meets clinical practice was the most significant factor in identifying clinically meaningful hazards with potential impact on patient care. In our analysis, the explicit models of clinical processes and the inherent traceability with the ePAM functions helped ensure that all associated Hazard Instances were identified and analysed in their clinical context. SMART does not allow a Hazard Instance to be declared without specifying the clinical process, step and setting within which it might occur. To achieve this, the existing medication processes had to be simplified in order to abstract detailed technology-oriented functions and focus on the clinical steps and context. These functions are important for system implementation but can often be a distraction when performing a clinically meaningful Hazard Identification.

Hazards on the Boundaries of Clinical Systems

ePAM covered two clinical systems: prescribing and allergies management. Hazards were identified on the outputs of these systems, e.g. 'wrong medication dose' or 'omission of an allergy in patient records'. However, distinguishing between technological factors and clinical factors proved a challenge. For example, when estimating the risk of a 'wrong medication', the clinicians estimated the totality of the risk and not just the risk due to non-clinical factors, i.e. which is the scope of the analysis. This issue highlights the difficulty of distinguishing between clinical and non-clinical factors in complex healthcare services, especially when HIT functions are intertwined with clinical processes. The ideal situation, though not realistic in this case, was to perform Hazard Identification and Risk Analysis on medication management as a clinical service and consider HIT as one of many factors. However, unfortunately, similar to the majority of HIT deployments, the sphere of control of the multidisciplinary team was the technology and its clinical context rather than the wider clinical practice. To some extent, the safety analysis had to be performed bottom up.

Sufficient Space for Detection and Mitigation

The hazards were defined in such a way that controls were specified in order to reduce the risk to acceptable levels. Most of these controls were already in place, e.g. training or supervision in clinical processes and tallman lettering for drug names. The results of the analysis did not generate any significant new controls, which might raise the questions as to whether the safety analysis was necessary. On reflection, the analysis was essential for two main reasons (excluding the need for compliance with SCCI 160). Firstly, the analysis clarified how HIT can compromise patient safety and highlighted the importance of the existing controls, i.e. the safety significance of certain practices and design features such as redundancy and cross-checking. Secondly, the analysis highlighted the need to monitor the effectiveness of the controls and the importance of revising the risk estimates based on real usage data. For example, making it hard for prescribers to use free text rather than use predefined drop-down lists is an existing control. It is now clear why it is important to regularly evaluate and monitor the extent to which prescribers are using the predefined list rather than free text.

Distinction between Hazards and Other Major Failures

Emphasising that hazards are specific events with specific characteristics was a challenge. Initially, the multidisciplinary team tended to label every significant event as a hazard. Their rationale was to ensure that the event was controlled. By calling an event a hazard, it was felt

that the hazard label elevated the significance of the event. However, this could result in unnecessarily large Hazard Logs. In the ePAM Hazard Identification, this issue was partly resolved by agreeing on Hazard Types prior to declaring Hazard Instances. This helped show that many failures that would otherwise be labeled as hazards were still specified and controlled as causes or effects. As discussed in Section 1, the source of this confusion is the generic definition of hazards as sources of patient harm.

Finally, the above observations, particularly the importance of the explicit traceability between the clinical setting, HIT functionality and hazards, potentially address the weaknesses reported by Habli et al [56] in their review of the Hazard Logs for 20 different HIT systems. Issues reported included confusing clinical hazards and HIT failures, with many hazards lacking a clear clinical impact and context. These issues made it difficult to assess the risk associated with the hazards and judge the suitability of the risk controls.

5.2 Overall Strengths and Weaknesses of SMART

Although the scope of the pilot study was limited to a specific setting and technology, it provided insights and highlighted practical challenges that will inform the future development and evaluation of the SMART.

Despite the additional clarity and automated support provided through SMART, hazard identification remains a complex task. This stems from the scale of healthcare, which is inherently a complex and adaptive sociotechnical system, and the uncertainty about actual practice, i.e. work-as-imagined vs work-as-done [52]. For example, estimating the likelihood and severity of the potential harms concerning a late prescription hazard in an Intensive Care Unit is extremely hard to perform. This is due to the sheer number of variables that have to be estimated, prior to the system deployment, concerning issues such as the medication type, the profile of the patients, the complexity of the clinical conditions and the state of the clinical setting. As such, proactive Hazard Identification and Risk Analysis is useful as long as it accompanied with a through-life safety management process that continuously updates and revises the clinical and technology models, and the associated Hazard Log, based on real-time usage data. That is, workarounds are common in healthcare. They often stem from the realities of complex clinical practice, which are hard to completely model prior to deployment. The continuous evaluation and updating of the clinical process models and their associated safety evidence is essential for maintaining the validity of the overall safety cases. One approach to achieving this, and reducing the gap between work-as-imagined vs work-as-done, is via the notion of dynamic safety cases [48] that supplement proactive safety analysis with reactive analysis of data collected from actual practices (e.g. via Bayesian Network [49]).
Further, the use of standard risk matrices for HIT, e.g. five likelihood ratings versus five severity ratings, seems to be too coarse to cater for the inherent risks that are due to the clinical conditions or the complexity of clinical decision making. That is, a difficulty was the fact that the likelihood and severity ratings seem to be "overall" as opposed to risk profiles that cater for combinations that cover high likelihoods of non-severe events and low likelihoods of severe events As such, the extent of the harms caused by the technology compared to those resulting from the clinical condition or disease is hard to determine. This highlights the need to explore alternative means for risk estimation for HIT, building on measures such as Quality-Adjusted Life-Years (QALYs) [53]. This also emphasises the importance of monitoring and collecting usage data in order to continuously revise the risk estimates and the underlying models of the clinical processes and settings.

A related important matter is risk proportionality. SMART provides clinicians and engineers with traceability data needed for analysing how the level of rigour and detail in the safety evidence is commensurate with the criticality of the clinical setting and HIT functionality. What is proportionate and therefore acceptable is a debatable and an ethically sensitive matter on which standards and legal systems have differed, i.e. similar to the discussion regarding the ‘As

Low As Reasonably Practicable' ALARP principle [47]. Most standards provide templates for risk matrices that distinguish between acceptable, tolerable and intolerable levels of risks [14, 16, 17]. Under exceptional circumstances, these standards allow engineers and clinicians to appeal to risk-benefit analysis to show that the clinical benefits outweigh the technological risks.

Our study provides further evidence concerning the importance of treating HIT safety assurance as a socio-technical process, involving both clinical and engineering stakeholders [13, 50]. This was exemplified in the difficulty of modelling the HIT functions given the variable nature of clinical settings; a significant issue that has been highlighted in the patient safety literature [51, 57] . The current literature on Resilience Engineering [58] and Safety 2.0 [59] emphasise the need to redefine the notion of variability. This is in order to help distinguish between, on the one hand, unsafe violations and, on the other hand, desirable performance adjustments that are necessary to ensure the ability of the system to maintain safety, given changing demands and disturbances. The Systems Engineering Initiative for Patient Safety (SEIPS 2.0) [51] also now more explicitly considers variability through the concepts of configuration and adaptation.

Finally, there are cultural challenges with risk analysis for HIT. On the one hand, many organisations still adopt a strategy of "*organisational ignorance*" [54] when it comes to HIT risks, and they rely almost exclusively on HIT suppliers to develop "safe" systems . On the other hand, and more positively, the introduction of the NHS Digital Academy with a remit to train clinical information officers can be seen as one instrument to bring about the required cultural change [55]. Further, many HIT systems are procured because of their perceived patient safety benefits. By identifying hazards that are posed by the system itself, safety analysis can be seen as introducing hurdles to the introduction of a technology that is intended to reduce medical errors. As such, more balanced debates are needed in order to identify, analyse and, where necessary, tradeoff clinical benefits and technological risks.

6 Conclusions

Current definitions of hazards are high level and generic. As such they are hard to interpret. This is particularly the case for large HIT systems used in complex socio-technical settings. Although hazard-directed safety processes are prominent in other safety-critical industries, the notion of hazards has to be refined and evaluated further in order to fit the complexity and scale of healthcare services. Publicly-available exemplar hazard logs and safety cases are needed in order to inform the debate concerning appropriate safety analysis approaches to HIT.

Two areas of further work are important: (1) further development of SMART in order to incorporate established socio-technical models such as SEIPS 2.0 [51] and (2) incorporating means for updating the clinical models and safety evidence dynamically based on real-time data. The combination of these two areas would help ensure that the safety analysis reflects the complex and adaptive sociotechnical realities of clinical practice and reduces the gap between work-as-imagined vs work-as-done.

Acknowledgements

This work was supported, in part, through a grant by the UK Royal Academy of Engineering (ISS1516\8\8). We are grateful to colleagues who supported SMART and this study: Alistair Morris, Kay Pagan, Paul Southern, Beve Smith, Jackie Murphy, Hannah Mccann, Wale Lawal, Chris McLernon and Damon Horn.

References

1. Black AD, Car J, Pagliari C, Anandan C, Cresswell K, Bokun T, McKinstry B, Procter R, Majeed A, Sheikh A. The impact of eHealth on the quality and safety of health care: a systematic overview. PLoS medicine. 2011 Jan 18;8(1):e1000387.
2. Agboola SO, Bates DW, Kvedar JC. Digital health and patient safety. Jama. 2016 Apr 26;315(16):1697-8.
3. Committee on Patient Safety and Health Information Technology. HIT and Patient Safety: Building Safer Systems for Better Care. National Academies Press; 2011.
4. Kapur N, Parand A, Soukup T, Reader T, Sevdalis N. Aviation and healthcare: a comparative review with implications for patient safety. JRSM open. 2015 Dec 2;7(1):2054270415616548.
5. Sujan MA, Habli I, Kelly TP, Pozzi S, Johnson CW. Should healthcare providers do safety cases? Lessons from a cross-industry review of safety case practices. Safety science. 2016 Apr 1;84:181-9.
6. Sujan, M.A., Koornneef, F., Chozos, N., Pozzi, S. and Kelly, T., 2013. Safety cases for medical devices and health information technology: involving health-care organisations in the assurance of safety. Health informatics journal, 19(3), pp.165-182.
7. Sujan, M.A., Koornneef, F. and Voges, U., 2007, September. Goal-based safety cases for medical devices: opportunities and challenges. In International Conference on Computer Safety, Reliability, and Security (pp. 14-27). Springer, Berlin, Heidelberg.
8. Niklas MÃ, Hansson SO, Holmberg JE, Rollenhagen C, editors. Handbook of Safety Principles. John Wiley & Sons; 2018 Jan 4.
9. SAE International. ARP4754A: Guidelines for Development of Civil Aircraft and Systems. SAE International: 2010.
10. Sujan MA, Habli I, Kelly TP, Gühnemann A, Pozzi S, Johnson CW. How can health care organisations make and justify decisions about risk reduction? Lessons from a cross-industry review and a health care stakeholder consensus development process. Reliability Engineering & System Safety. 2017 May 1;161:1-1.
11. Vincent C, Amalberti R. Safety in healthcare is a moving target.
12. Vincent C. Patient safety. BMJ Books; 2010.
13. Sittig DF, Singh H. A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. BMJ Quality & Safety. 2010 Oct 1;19(Suppl 3):i68-74.
14. NHS Digital. SCCI0160, Clinical Risk Management: its Application in the Deployment and Use of HIT Systems. Standardisation Committee for Care Information; 2016
15. Magrabi F, Ong MS, Runciman W, Coiera E. An analysis of computer-related patient safety incidents to inform the development of a classification. Journal of the American Medical Informatics Association. 2010 Nov 1;17(6):663-70.
16. ISO. ISO 14971 Risk management for medical devices. ISO.2010.
17. IEC. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES). IEC; 2010.
18. Federal Aviation Administration. FAA Integrated Oversight Philosophy. FAA, 2017.
19. Ministry of Defence: Defence Standard 00-56 Safety Management Requirements for Defence Systems. Ministry of Defence. 2007.
20. Leveson N. Engineering a safer world: Systems thinking applied to safety. MIT press; 2011.
21. Althaus, C. E. 2005. A disciplinary perspective on the epistemological status of risk. Risk Analysis, 25, 567-588.
22. AVEN, T. 2011. On the new ISO guide on risk management terminology. Reliability Engineering & System Safety, 96, 719-726.
23. Ferdous R, Khan F, Sadiq R, Amyotte P, Veitch B. Analyzing system safety and risks under uncertainty using a bow-tie diagram: an innovative approach. Process Safety and Environmental Protection. 2013 Jan 1;91(1):1-8.
24. Vesely WE, Goldberg FF, Roberts NH, Haasl DF. Fault tree handbook. Nuclear Regulatory Commission Washington DC; 1981 Jan.
25. Object Management Group. Unified Modeling Language. OMG; 2017.
26. Carayon P, Hundt AS, Karsh BT, Gurses AP, Alvarado CJ, Smith M, Brennan PF. Work system design for patient safety: the SEIPS model. BMJ Quality & Safety. 2006 Dec 1;15(suppl 1):i50-8.
27. Singh H, Sittig DF. Measuring and improving patient safety through health information technology: The Health IT Safety Framework. BMJ Qual Saf. 2016 Apr 1;25(4):226-32.

28. Steinberg D, Budinsky F, Merks E, Paternostro M. EMF: eclipse modeling framework. Pearson Education; 2008 Dec 16.
29. Elliott R, Camacho E, Campbell F, Jankovic D, Martyn St James M, Kaltenthaler E, Wong R, Sculpher M, Faria R. Prevalence and economic burden of medication errors in the NHS in England. Rapid evidence synthesis and economic analysis of the prevalence and burden of medication error in the UK. 2018.
30. Donyai P, O'grady K, Jacklin A, Barber N, Franklin BD. The effects of electronic prescribing on the quality of prescribing. British journal of clinical pharmacology. 2008 Feb 1;65(2):230-7.
31. Ash JS, Sittig DF, Dykstra RH, Guappone K, Carpenter JD, Seshadri V. Categorizing the unintended sociotechnical consequences of computerized provider order entry. International journal of medical informatics. 2007 Jun 1;76:S21-7.
32. Fook J. Developing critical reflection as a research method. InCreative spaces for qualitative researching 2011 (pp. 55-64). SensePublishers.
33. Stake RE. The art of case study research. Sage; 1995 Apr 5.
34. Grissinger M. The five rights: a destination without a map. Pharmacy and Therapeutics. 2010 Oct;35(10):542.
35. NHS Improvement. Rationale for not including Never Events proposed through consultation in the Never Events list 2018. NHS Improvement; 2018.
36. MHRA and NHS England. Improving medication error incident reporting and learning. NHS/PSA/D/2014/005; 2014
37. NICE. Drug allergy: diagnosis and management. Clinical guideline [CG183]; 2014.
38. Pumfrey DJ. The principled design of computer system safety analyses (Doctoral dissertation, University of York).
39. Redmill F, Chudleigh M, Catmur J. System safety: HAZOP and software HAZOP. Chichester: Wiley; 1999 Oct.
40. Sujan MA, Felici M. Combining failure mode and functional resonance analyses in healthcare settings. InInternational Conference on Computer Safety, Reliability, and Security 2012 Sep 25 (pp. 364-375). Springer, Berlin, Heidelberg.
41. Pasquini, A., Pozzi, S. and Save, L., 2011. A critical view of severity classification in risk assessment methods. Reliability Engineering & System Safety, 96(1), pp.53-63.
42. Aronson JK. Medication errors: what they are, how they happen, and how to avoid them. QJM: An International Journal of Medicine. 2009 Aug 1;102(8):513-21.
43. Velo GP, Minuz P. Medication errors: prescribing faults and prescription errors. British journal of clinical pharmacology. 2009 Jun 1;67(6):624-8.
44. McDermid JA, Pumfrey DJ. A development of hazard analysis to aid software design. InComputer Assurance, 1994. COMPASS'94 Safety, Reliability, Fault Tolerance, Concurrency and Real Time, Security. Proceedings of the Ninth Annual Conference on 1994 Jun (pp. 17-25). IEEE.
45. Marcin JP, Dharmar M, Cho M, Seifert LL, Cook JL, Cole SL, Nasrollahzadeh F, Romano PS. Medication errors among acutely ill and injured children treated in rural emergency departments. Annals of emergency medicine. 2007 Oct 1;50(4):361-7.
46. Dharmar M, Kuppermann N, Romano PS, Yang NH, Nesbitt TS, Phan J, Nguyen C, Parsapour K, Marcin JP. Telemedicine consultations and medication errors in rural emergency departments. Pediatrics. 2013 Dec 1;132(6):1090-7.
47. Health and Safety Executive. Reducing Risks, Protecting People. HSE, 2001..
48. Denney E, Pai G, Habli I. Dynamic safety cases for through-life safety assurance. In 2015 IEEE/ACM 37th IEEE International Conference on Software Engineering 2015 May 16 (Vol. 2, pp. 587-590). IEEE.
49. Denney E, Pai G, Habli I. Towards measurement of confidence in safety cases. In 2011 International Symposium on Empirical Software Engineering and Measurement 2011 Sep 22 (pp. 380-383). IEEE.
50. Meeks DW, Takian A, Sittig DF, Singh H, Barber N. Exploring the sociotechnical intersection of patient safety and electronic health record implementation. Journal of the American Medical Informatics Association. 2013 Sep 19;21(e1):e28-34.
51. Holden RJ, Carayon P, Gurses AP, Hoonakker P, Hundt AS, Ozok AA, Rivera-Rodriguez AJ. SEIPS 2.0: a human factors framework for studying and improving the work of healthcare professionals and patients. Ergonomics. 2013 Nov 1;56(11):1669-86.
52. Blandford A, Furniss D, Vincent C. Patient safety and interactive medical devices: realigning work as imagined and work as done. Clinical risk. 2014 Sep;20(5):107-10.

53. Torrance GW, Feeny D. Utilities and quality-adjusted life years. International journal of technology assessment in health care. 1989 Oct;5(4):559-75.
54. Sujan, M.. Managing the patient safety risks of bottom-up health information technology innovations: recommendations for healthcare providers. Journal of Innovation in Health Informatics. 2018; 25(7).
55. Sood H, NcNeil K, Keogh B. Chief clinical information officers: clinical leadership for a digital age. BMJ: British Medical Journal (Online). 2017 Jul 10;358.
56. Habli I, White S, Sujan M, Harrison S, Ugarte M. What is the safety case for health IT? A study of assurance practices in England. Safety Science. 2018 Dec 1;110:324-35.
57. Vincent C, Amalberti R. Safety in healthcare is a moving target.
58. Hollnagel E, Braithwaite J, Wears RL, editors. Resilient health care. Ashgate Publishing, Ltd.; 2013 Sep 2.
59. Hollnagel E. Safety-I and safety-II: the past and future of safety management. CRC Press; 2018 Apr 17.